OUTLINE SHEET 5.8

Dissemination, Visits and Meetings

REFERENCES

SECNAV M-5510.36 (Chapters 2, 7, 8, & 11)
SECNAV M-5510.30 (Chapters 1, 9 & 11)
DOD Directive 5210.2, Access to and Dissemination of Restricted Data
SECNAVINST S5460.3C, Management, Administration, Support, and Oversight of Special Access Programs within Department of the Navy (U)
DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM)
DOD 5220.22-M Supp 1, NISPOM Supplement 1
SECNAVINST 5510.34A, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives
DOD Directive 5230.24, Distribution Statements on Technical Documents
OPNAVINST 5510.161, Withholding of Unclassified Technical Data from Public Disclosure
SECNAVINST 5430.107, Mission and Functions of the Naval Criminal Investigative Service
DOD 5105.21-M-1, DOD Sensitive Compartmented Information Administration Security Manual

OUTLINE

A. Basic Policy For Dissemination Of Classified Information and Controlled Unclassified Information (CUI) (ISP 8-1)

1. COs shall establish procedures for the dissemination of classified and CUI originated or received by the command to include:

   - Release classified information only when need-to-know has been demonstrated
   - Reflect releasing restrictions imposed by the originator or higher authority

2. Disclosure of classified information to an individual(s) not eligible may be approved by SECNAV in emergency situations in which there is an imminent threat to life in defense of the homeland (see paragraph 8-1-4 PSP for details)

B. Dissemination Procedures: (ISP 8-1 THRU 8-4)

1. Top Secret originated within DOD - Originator/higher authority must approve dissemination outside DOD (except in emergency situation in defense of homeland, paragraph 8-1.4 PSP)

2. Secret and Confidential originated within DOD - Can be disseminated within Executive Branch, unless prohibited by originator (except in emergency situation in defense of homeland, paragraph 8-1.4 PSP)

3. Originated in a non-DOD department or agency - Do not disseminate outside DOD without consent of originator department/agency ("third agency rule")

4. Special Access Program (SAP) Information **(PSP 1-7)**

   a. Programs requiring additional security measures in addition to those for Top Secret, Secret and Confidential

   b. Regulated within DON by SECNAVINST S5460.3C

5. Restricted Data (RD) (including Critical Nuclear Weapon Design Information (CNWDI)) **(ISP 8-4, PSP 9-19)**

   a. Defined as data concerning: Design manufacture or utilization of atomic weapons; Production of special nuclear material; Use of special nuclear material in production of energy

   b. Within DOD - Can be disseminated unless specifically prohibited

   c. Outside DOD – Refer to DOD Directive 5210.2

   NOTE: Dissemination of CNWDI should be of special concern due to extreme sensitivity of this information (For additional guidance see paragraph 9-19 PSP)

6. Special Programs **(PSP 1-6, ISP 8-4)**

   a. Any program requiring additional security protection and handling measures, reporting procedures or formal access lists

   b. Regulated by a variety of directives that give particular guidance for dissemination, these programs include:

- North Atlantic Treaty Organization (NATO)
- Nuclear Command and Control – Extremely Sensitive Information (NC2-ESI)
- Nuclear Weapon Personnel Reliability Program (PRP)
- Naval Nuclear Propulsion Information (NNPI)

7. Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) **(ISP 8-4)**

   a. Have dissemination controls additional to SECNAV M- 5510.36 and M-5510.30 requirements

   b. Special Security Officer (SSO) is responsible for SCI material

   c. Electronic Key Management System (EKMS) Manager is responsible for COMSEC material

8. Controlled Unclassified Information **(ISP 8-4)**

   The following categories of unclassified information may have limits on dissemination and/or may require special markings prior to dissemination:

   - For Official Use Only (FOUO)
   - Sensitive But Unclassified (SBU)
   - DEA Sensitive Information/Material
   - DOE Unclassified Controlled Nuclear Information (DOE UCNI)
   - DOD Unclassified Controlled Nuclear Information DOD UCNI)

C. Dissemination Through Judicial Proceedings (PSP 9-11)

1. Chapter 9, 5510.30A outlines specific procedures for requesting authorization for civilian attorneys representing DON personnel who require access to classified information to adequately represent clients and for witnesses and visitors requiring access

2. Advise all command personnel that classified information may not be disclosed in any legal proceeding without appropriate authorization

D. Dissemination of Classified Information To DOD Contractors

1. Basic Policy

a. CO responsibilities **(ISP 11-1)**

(1) Establish an Industrial Security Program if command does classified procurement and/or has cleared contractors working in areas under their direct control

(2) Ensure command security procedures include appropriate guidance on safeguarding of classified information released to contractors

b. National Industrial Security Program (NISP) operates under DOD 5220.22-M and 5220.22-M Supplement 1 (SCI supplement) **(ISP 11-2)**

(1) Prescribes procedures to safeguard classified information (including special types of information) released to government contractors

(2) SECNAV M-5510.36 implements NISP requirements within DON

c. Defense Security Service (DSS) **(ISP 11-3)**

(1) Oversees DOD implementation of NISP through 5 regions comprised of field offices located throughout the U.S.

(2) Provide administrative assistance and policy guidance to DSS field offices charged with security oversight of cleared DOD contractors that perform on classified contracts

(3) Defense Industrial Security Clearance Office (DISCO):

- Grants Contractor personnel security clearances (PCLs) and facility security clearances (FCLs)
- Processes overseas visit requests
- Responds to requests regarding PCL and FCL applications and facility safeguarding capability

(4) DSS's homepage http://www.dss.mil provides additional information on DSS functions

2. Disclose classified information only if contractor: **(ISP 11-8)**

   a. Is cleared under NISP and requires access in connection with a legitimate U.S. government requirement

   b. Has valid FCL and storage capabilities - Written verification (valid for 3 years) of FCL level and storage capability provided by DSS/OCC Central Verification Activity (CVA) or contractor's OPLOC

      - FCL in JPAS Person Summary under "Organization Status" or
      - Contact CVA via e-mail at discofac@dislink.jcte.jcs.mil or phone 1-888-282-7682 for verification

   c. Overseas – Commands must first take the following additional security measures:

      (1) Verify that requirement for access overseas is essential to contract

      (2) Require classified information provided to cleared contractor is stored at a U.S. government controlled facility or military installation – unless a written waiver or exception granted by CNO (N09N2)

      (3) Provide overseas installation commander and responsible DSS/OPLOC with:

         - Notice of contract award
         - Any special instructions (e.g., transmission, storage, disposition)
         - Copy of original DD 254

3. DOD Contract Security Classification Specification (DD 254) (See Student CD for DD 254 Form) **(ISP 11-10)**

   a. Required for each classified contract - Prepared by command awarding contract

   b. Provides contractor with security requirements and classification guidance for performance

4. Contracting Officer Representative (COR) **(ISP 2-6, 11-5)**

a. Qualified security specialist appointed, in writing, by commands that award classified contracts

b. Responsible for completion, signing and oversight of DD 254

c. Verifies contractor PCLs and FCLs

d. Responsible to security manager for coordination with program manager and procurement officials

e. Ensures the NISP functions specified in the ISP are accomplished

NOTE: Paragraph 11-5 SECNAV M-5510.36 contains a complete listing of COR's duties

5. Security Oversight of Cleared Contractor Operations **(ISP 11-4)**

a. Shipboard – Cleared contractors will:

- Have visitor status
- Conform to command security regulations
- Submit visit requests using JPAS to CO and receive approval for classified visits to any U.S. Navy ship

b. Shore – Contractors may perform work on and visit shore installations in one of the following ways:

(1) When CO determines contractor is a short or long-term visitor – CO shall require visitor comply with command security regulations and be included in command security education program

(2) When contractor is a tenant the host command may assume responsibility for security oversight – Contractor is obligated to comply with DON regulations

(3) CO may request, in writing, that DSS grant contractor an FCL and assume security oversight – in which case CO has no authority over the contractors' employees or occupied spaces

c. Off-site locations – When contractor performs work at location other than contract awarding command. Command will inform new host and provide host copies of contract award notification, DD 254 and other pertinent documents:

d. DON overseas locations

(1) Contractor and his/her employees will be considered visitors and will follow security guidelines established by host command DSS

(2) Host command will furnish security requirements to the visitors

6. Releasing Intelligence to Contractors – Director, Office of Naval Intelligence (ONI) (ONI-5) is responsible for executing the policy and procedures governing the release of intelligence to cleared DOD contractors and is the final appeal authority on release denial **(ISP 11-13 and 11-14)**

7. DO NOT publish/disclose privately owned proprietary information (e.g., trade secrets, processes, statistics, etc.) without written permission of the legal owner or proprietor **(ISP 11-9)**

NOTE: Controlled Unclassified Information can be released to a contractor with a need-to-know consistent with the requirements of the contract unless there are any restrictions identified **(ISP 11-9)**

E. DISCLOSURE TO FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS (ISP 8-1, PSP 9-16)

1. Governing instruction - SECNAVINST 5510.34A

2. No information will be disclosed unless specifically authorized in writing per SECNAVINST 5510.34A

3. Navy International Programs Office (Navy IPO) – Centralized authority for disclosure of classified information to foreign governments

4. U.S. citizen officials/employees of foreign governments, firms, etc. are considered to be representing a foreign government (when acting in that capacity)

5. Personnel Exchange Program (PEP) billets - If command has foreign nationals on staff in Personnel Exchange Program (PEP) billets – must be aware of provisions of SECNAVINST 5510.34A

6. Admission of foreign nationals to classified courses or training requires approval of Navy IPO

7. Scrupulously limit degree of access by representatives of foreign governments, including PEP personnel, to that allowed by Foreign Disclosure Authorization issued by Navy IPO on a case-by-case basis

NOTE: Navy IPO phone numbers (DSN 764)
Foreign Disclosure: (202) 764-2380/2374
PEP: (202) 764-2383/2384
Fax: (202) 764-2465
Website: https://www.nipo.navy.mil

F. Dissemination Of Technical Documents (ISP 8-7, Exhibit 8A)

1. Technical documents require distribution statements to facilitate control, distribution and release without constant referral to originator.

   a. Technical document - Any recorded information that conveys scientific and technical information or technical data.

   b. Technical information – Information, including scientific information, that relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.

   c. Technical data – Recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material

   d. Distribution Statements:

      A: Approved for public release; distribution is Unlimited

B: Distribution authorized to U.S. Government agencies only; (fill in reason) (date). Other requests for this document must be referred to (insert originating command)

C: Distribution authorized to U.S. Government agencies and their contractors; (fill in reason) (date). Other requests for this document will be referred to (insert originating command)

D: Distribution authorized to DOD and DOD contractors only; (fill in reason) (date). Other U.S. requests shall be referred to (insert originating command)

E: Distribution authorized to DOD components only; (fill in reason) (date). Other requests must be referred to (insert originating command)

F: Further dissemination only as directed by (insert originating command) (date) or higher DOD authority

X: Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with OPNAVINST 5510.161. Other requests must be referred to (originating command).

2. Command originating or responsible for a technical document must:

   a. Determine its availability for distribution, release, and dissemination without additional approval or authorization (secondary distribution)

   b. Mark it accordingly: *Unclassified* technical documents require distribution statements; *classified* technical documents must be assigned distribution statement B, C, D, E, or F

3. Detailed guidance on use of these statements is given in paragraph 8-7 and exhibit 8A, SECNAVINST 5510.36

4. Distribute technical data in your possession as indicated in its distribution statement

G. Prepublication Review (PSP 8-8 and Exhibit 8B)

1. DOD policy - A security and policy review shall be performed on all official DOD information intended for public release **including** placement on publicly accessible websites or computer servers

2. Documents proposed for public release will first be reviewed at command level and if found suitable for public release can be released without higher-level consideration

   a. COs are authorized to release information to the public that is wholly within the command mission and scope

   b. Each CO is responsible for ensuring that a review of the material proposed for public release is completed (normally PAOs job but coordinated through the Security Manager)

3. If public release cannot be authorized within the chain of command – the material must be submitted for further review to CNO (N09N2) for Navy commands or CMC (ARS) for USMC commands

   a. Exhibit 8B, PSP identifies official DOD information prepared by or for DOD personnel and proposed for public release that requires further review by the DOD Office of Security Review (DOD OSR) via CNO (N09N2)

   b. DOD OSR coordinates prepublication review with the cognizant authorities outside DON and provides final determination for public release

H. Basic Policy For Visit Control (PSP 11-1)

1. For security purposes, a "visitor" is a person for whom you do not have security jurisdiction who seeks access to classified information under your security control

2. Responsibilities of CO of the activity being visited

   a. Ensure visitors have appropriate level of security clearance and need-to-know

b. Ensure movement of visitors is consistent with purpose of visit (If escort required – May use cleared and properly trained military, civilian or contractor assigned to command being visited)

3. General visiting – allowed on unclassified basis only – written statement of command safeguards will be implemented (i.e., General Visiting Bill)

I. Classified Visits (PSP 11-2)

1. COs shall establish procedures to accommodate visits to their commands involving access to, or disclosure of, classified information.

   a. As a minimum these procedures will include checking JPAS for:

      - Verification of identity
      - Validation of security clearance eligibility
      - Documentation of access
      - Currency and accuracy of affiliation data

   b. Once JPAS verified, command must determine need-to know of visitor

2. Visitor's commands are responsible for ensuring visitor's eligibility, access and affiliation data are current and accurate in JPAS

3. If local conditions necessitate formal visit request letters for visit/access control purposes, the command sponsoring the visitor must comply with local facility access. If the visit request is not sent through JPAS, a formal visit request should include the following information:

      - Full name; rank, rate or grade; date and place of birth; SSN; title; position; UIC/RUC and citizenship of the proposed visitor
      - Employer or sponsor, if other than originator
      - Name and address of activity to be visited, if other than addressee
      - Date and duration of proposed visit
      - Purpose of visit in detail, including estimated degree of access required
      - For special authorization access (e.g., NATO, NC2-ESI), the visiting command confirms that the visitor has been briefed and authorized such

access
- Security clearance status of visitor (basis of clearance is not required)
- Where appropriate, names of persons to be visited

NOTE: The visit request must be submitted in advance, individuals can never handcarry their own visit request

4. Visits by DOD contractors – The same procedures apply for contractors as are listed above in paragraphs 1 – 3, except a formal visit from a contractor will also require the identification of their facility clearance

NOTE: Facility clearance in JPAS is listed "Organization Status" on the Person Summary

J. Visitor Identification (PSP 11-1)

1. A visitor authorized access to classified information must provide: ID card with recognizable photograph, name, and signature (CAC cards do not have a signature but are an official government ID and can be accepted)

2. Flag Officers, general officers, and civilian equivalents are not required to sign visitor records or display ID badges when being escorted as visitors. (If not escorted, they must comply with all normal security procedures)

3. Personnel issued NCIS Special Agent credentials are cleared for access up to and including Top Secret. They shall be presumed to have a need-to-know with regard to access to information, material, or spaces relevant to the performance of their official duties. Authority for access to special intelligence and Compartmented or similarly controlled spaces, will be requested. **(SECNAVINST 5430.107)**

K. Visits By Members Of Congress (PSP 11-4)

1. Normally arranged by Office of Legislative Affairs (OLA) or other Navy Department officials

2. No clearance required for members of Congress; but clearance eligibility is required for staff members

3. *No final refusal to furnish classified information will be made by a CO.* The case will be referred to SECNAV

through OLA

L. Visits By Foreign Nationals (PSP 11-3)

1. Visits by foreign nationals and representatives of foreign governments, foreign industry or international organizations:

   a. Must be approved by the Navy International Programs Office (Navy IPO) or an authority specifically delegated in SECNAVINST 5510.34A

   b. Disclosure level for classified information (if required) determined for each visitor

2. Official visit requests must be submitted by applicable foreign government certifying visitor's national clearances and need-to-know

3. CO may invite or permit courtesy calls and general visiting

M. Basic Policy For Classified Meetings (ISP 7-13)

1. Gatherings considered to be "meetings" include conferences, symposia, exhibits, conventions, seminars, training courses, etc.

2. Classified meetings shall be held only:

   - If disclosure of information serves a specific U.S. government purpose
   - At a U.S. government or cleared DOD contractor facility (no exceptions)
   - Where adequate physical security and procedural controls have been approved

N. Security Sponsorship (ISP 7-13)

1. Commands conducting/hosting "in-house" classified meetings attended by command members and/or authorized visitors shall assume security responsibility (sponsorship)

2. If your command allows another to use its spaces for a classified meeting but does not accept security sponsorship, you must apprise that command that it is responsible

3. Commands hosting meetings outside command, including

those supported by non-government associations, will:

a. Confirm other means to communicate the information are inadequate and ensure attendance limited to:

- U.S. government personnel
- Cleared DOD contractors
- Foreign government personnel with appropriate clearance/need-to-know

NOTE: Any participation by foreign nationals or foreign representatives must be approved in writing by Navy IPO prior to attendance and information to be presented cleared for foreign disclosure

b. Implement security plan that minimizes risk to classified material

c. Segregate classified from unclassified sessions

d. Ensure announcements unclassified and information limited

e. Safeguard, transmit, or transport classified information per SECNAVINST 5510.36

f. Permit note taking or electronic recording during classified sessions **only** if sponsor agrees in writing it is necessary

4. CNO (N09N2) approval required before commitment to or announcement of classified meetings when:

a. Commands invited to make classified presentations or to accept security sponsorship for classified meetings organized by non-U.S. government associations

b. Format for submitting approval request is in SECNAV M-5510.36, paragraph 7-13.4 (If request approved, CNO (N09N2) will designate security manager for the meeting)

c. Pending CNO (N09N2) decision, general notices or announcements of meetings may be published or sent out if it does not constitute invitation to attend